The Bill Blackwood
Law Enforcement Management Institute of Texas

==========

Can Cyber Crimes Be Prevented?

==========

An Administrative Research Paper
Submitted in Partial Fulfillment
Of the Requirements for Graduation from the
Leadership Command College

==========

by
Michael A. Bland

Midwestern State University Police Department
Wichita Falls, Texas
February 2002

ABSTRACT

The computer has rapidly become a necessity in today's society. It can no longer be considered a luxury if one is to stay competitive. If "information is power, II then the one who controls the most information is most powerful. As long as people are willing to seek an advantage over others, they will be seeking information. Once this information is obtained, how can it be safeguarded? Once a compromise has been detected how does one go about investigating an incident and establishing sufficient probable cause for prosecution?

A survey of various law enforcement agencies was made. The survey asked if training in the investigation of computer related offenses had been received by individuals of their departments and the level of confidence felt in their ability to investigate the offense without the assistance of an outside agency. The survey indicated a lack of confidence by most departments and the need for more specialized training in the field of cyber investigation. A new challenge is facing law enforcement on the cyber frontier; only with education and training equal to or greater than that of the perpetrator can this challenge be met.

It is concluded that cyber crimes cannot be prevented anymore than any other type of crime can be. Deterrence is all that can be offered. Until the measures required for the prevention appear to be worthwhile, they may never be deemed practical or realistic to the individual or organizations due to the cost and time restraints required for implementation.

TABLE OF CONTENTS

INTRODUCTION

The computer lends itself easily to criminal abuse. It is a willing accomplice. Computers can be used to pilfer and or manipulate both information and funds. As the availability of computers increase so does the opportunity for computer related offenses. Computer related offenses often go un-detected, they are crimes of stealth with no witnesses. Even an experienced investigator, without proper training has no idea where to begin in the collection and preservation of evidence From an electronic medium.

A survey of over forty law enforcement agencies was made. Questions were asked as to whether or not any persons in their departments received training in the investigation of cyber crimes. The departments were then asked to rate the confidence level of being able to investigate a cyber crime in a satisfactory or unsatisfactory manner.

Larger departments having a greater pool of resources were expected to demonstrate a higher level of confidence in their ability to investigate a cyber offense without assistance from an outside agency. Personnel trained in cyber related offenses were expected to be more proficient and demonstrate a higher level of confidence in the investigation of a cyber related offense.

Research will show even departments with trained personnel in cyber investigation do not feel they could adequately investigate a cyber crime without outside agency assistance. This has resulted in the pooling of resources and the creation of *Task Forces*, where resources are consolidated and shared. Often times a department will yield concurrent jurisdiction of the cyber offense to state or federal level due to the lack of resources.

REVIEW OF LITERATURE

In 1995, a twenty-eight year old Russian biochemistry graduate student in Saint Petersburg, Russia used sophisticated computer codes to break into New York Citicorp's computerized cash-management system. He transferred more than twelve million dollars to banks around the world and had access to Citicorp's daily transfer of five hundred billion dollars (Carley & O'Brien, 1995). Only through the initiatives of the Federal Bureau of Investigation and cooperation from the Russian police and law enforcement agencies of four continents was it made possible to prevent a catastrophe, which eventually resulted in an arrest. According to the February 1995 edition of the National Military Strategy of the United States, one of the goals of the strategy for flexibility and selective engagement is to "win the information war". (Thomas, 1997) The National Defense University's School of Information Warfare and Strategy defines "information warfare" as:

Actions taken to preserve the integrity of one's own information systems from exploitation, corruption, or destruction while at the same time exploiting, corrupting, or destroying an adversary's information system and in the process achieving an information advantage in the application of force.

There are a number of basic fraud indicators to which management should be aware. Recognizing them requires little or no technical knowledge or training. However, being able to identify these indicators, management can play an important role in safeguarding an organization's computer from unauthorized use and abuse. The prevention and detection of computer related thefts and abuses should be a concern of every organization. Management should understand the conditions and environment that give rise to such offenses. Managers need to be trained and educated to both identify and help in solving such problems. Managers

need not become experts in the field of computer security any more than they need to become experts in other fields that may have an impact on their organization. Unfortunately, too many organizations believe if they close their eyes the problem will go away. Instead this only makes it easier for theft and abuse by the computer user.

Motive is the "why" behind a crime, the impulse, emotion or desire that leads a person to do something. It is not always essential to establish a motive to charge someone with a crime. For example, if you are in a restaurant and you observe an individual pull out a pistol and shoot their dining companion, it is not necessary to show why they did it. You and the dozen other eyewitnesses observed the incident take place, and that is all that is needed to convict. Cyber crimes unfortunately, are seldom that easy. Cyber crimes are often a crime of stealth, the perpetrator is rarely observed in the act of committing the crime. Before a cyber crime can be prosecuted, someone has to come forth and be a witness. It is the witness who provides authorities with sufficient information to conduct a successful investigation. Thus, the role of the witness is an important one. Many computer crimes surface only when a witness comes forth. The witness then becomes the center of the criminal investigation. Witnesses have not always been treated fairly by our criminal justice system. Society looks upon them with suspicion, and their fellow employees view them as ones not to be trusted. So it is helpful for prosecutors to establish some type of a motive. Some cyber crimes are rational: the perpetrator stands to gain something. It could be something tangible, such as money. Or what the perpetrator wants could be intangible: revenge, attainment of a goal, or support of a cause. Other motives can seem irrational. There seemingly is no logical reason for the crime, and the perpetrator stands to gain nothing. To establish possible motives and develop suspects, one must interview persons who

would have knowledge about the crime or how to commit one. Besides their knowledge of how the crime was committed, they might provide other important details.

Who is this perpetrator that can cause both the government and private industry such great and justifiable concern? If one is to understand and address the problem of the cyber criminal, one must understand what motivates them. Unlike other crimes, the lower socio-economic strata of our society do not usually commit cyber crimes. Salaried or professional persons in conjunction with their work typically commit cyber crimes. Cyber crimes are not the result of depravity. They are the calculated acts of professional persons who occupy positions of trust and are armed with the most modern technology of our society usually entrusted to them. They are crimes committed by our *technocratic class,* persons who operate, program, and service our automated systems and are referred to as white-collar crimes.

The typical cyber criminal can be profiled accordingly. They are usually between the age of fifteen and forty-five years old. Males commit most of the crimes, but as more females enter the work force, more females are becoming more involved. (Guy, 2000) They have no previous criminal history and posses a technical background, even if limited to just the operation of the computer. They would be the last persons one would suspect of committing a criminal act. The individual fears exposure, ridicule and loss of status within the community and seeks to justify their criminal act by viewing it as just a “game.” (White Collar Crime, 1992) The perpetrator is normally employed in a position of trust with easy access to the computer and does little to deviate from the accepted norms of society. They are usually on guard about their activities and typically are the first to arrive at work and the last to leave. They take few or no vacations and normally work alone. (Bequai, 1983)

Up until recently, neither the public nor our criminal justice system viewed the cyber criminal as a threat to society. With computer security being lax or nonexistent, the compromise of information systems is often easily corruptible. Management often unknowingly aids the cyber criminals. Few computer criminals are ever referred to a prosecutor. Many cyber crimes are swept under the carpet; the losses are typically passed on to the consumer or taxpayer. If the violation results in the loss or damage of information, the victim usually does not want it to be publicized. It is no secret that management is often reluctant to prosecute computer crimes. The perpetrator, when caught, is usually dismissed or transferred to another department. A reluctance to prosecute can hardly be said to serve as a deterrent, it usually only serves to tell 'others to *try* their hand.

The victim, should not always be faulted, various circumstances often result in their decision. The victim's decision may be decided by the idea of cyber crimes not being considered he same as street crime. The detection and prosecution of computer crimes often tasks the limited resources of an organization. The police often must rely on the assistance of the perpetrators for successful prosecution. (White-Collar Crime, 1992) Further the victim's business operation may be affected, as employees, records, and equipment may find their way to court as evidence or witnesses. The public unfortunately often views the victim as foolish, stupid and careless, almost as if inviting the crime. The public sheds very few tears for a corporation or government agency that falls victim to a cyber crime. Failure of management to take adequate measures to secure and safeguard computer files could raise the possibility of lawsuits by stockholders.

Two possible areas of abuse that should cause managers special concern are *unauthorized access* and *misuse of the system.* (White-Collar Crime, 1992) These two categories of abuse

threaten the accuracy, integrity and reliability of the data stored within the system. Unauthorized access can be achieved by one or more of the following: theft of an authorized user's password or file name, manipulating or the changing of part of the program, gaining control of the system, removal of the storage device, or exploiting access privileges.

Misuse of a computer system is more prevalent than unauthorized access. The misuse of a system can be the result of authorized users engaging in activities by the use of a modem or remote terminal. They can remove, modify or change components and information of the system without notice or alarm for concern. The tampering or removing of components from the computer system can greatly affect the efficiency of the system and cause loss of data or complete system failure. Monitoring the activities of authorized users can prove difficult or next to impossible. Authorized users should also be viewed as potential suspects when computer misuse is suspected.

The potential for abuse of a computer system not only comes from employees, but also From personnel who are employed to maintain, service, and operate the system. Law enforcements ability to identify potential threats to the system can often play an important role in the detection of cyber crimes and other related offenses. Equally important, law enforcement should be able to anticipate and address the potential threats to a cyber system. This is not always an easy task, and often requires more extensive training and experience.

If evidence of a computer failure is present, one should first determine the extent and nature of the problem. Find out if the incident was accidental or intentional. Could it have been caused by operator, hardware or software error? Alternatively, could it have been caused by some natural phenomena such as a power surge or loss of power?

Next one should record the events once it has been decided the act was intentional. This

can be considered as part of interviewing suspects and knowing the right questions to ask. It is important to remember interviewing and interrogation are two separate techniques. After zeroing in on a suspect, a list of system personnel by job description should be compiled. This can help determine if the suspect had the opportunity to commit such an offense.

While handling the investigation, be sure to guard against violating or abusing the privacy rights of both the witnesses and suspects. Abuse of these rights could result in a successful civil lawsuit against the organization or persons doing the investigation. Finally prepare a report of managements findings. A detailed summary of the facts of the case in chronological order should be done. At a minimum it should include a summary of potential testimony each witness is willing to give, the name and job description of each witness and suspect, and a list of available evidence and losses suffered

METHODOLOGY

Can cyber crimes be prevented? It is argued that cyber crimes can be prevented, although the effort and precautions necessary may not be deemed worthwhile to the individual or business entity until after they have fallen victim to what was once called a victimless crime. It is believed in order to deter cyber crime police should receive specialized training in areas of safeguarding cyber related evidence. To examine this issue fifty-six surveys were sent to various individuals employed with various law enforcement agencies in the state of Texas. The respondents were participants of Phase I and Phase II of the Leadership Command College at Texas A & M University and Texas Women's University. Of the fifty-six surveys solicited, all were returned for consideration. When survey information was collected from respondents from the same agency the information was scrutinized for conflicting results. Once redundant surveys

were removed, this resulted in a core survey of forty departments. The departments were asked to rate the confidence level of their ability to investigate a cyber crime in a satisfactory or unsatisfactory manner and whether personnel in their departments had any type of special training geared toward cyber crime investigation. Other factors were given into consideration as to the authorized number of commissioned officers, the population of the jurisdiction they represented and whether they were a state, municipal, county, university, school district or other.

FINDINGS

The agencies surveyed ranged in size from nine to over eleven hundred commissioned officers. The respondents were of staff level representing six county sheriff s departments, twenty-six city municipalities, three universities, three independent school districts and the other category, consisting of the Texas Commission on Law Enforcement Standards and Education and an airport department of public safety. The departments surveyed all recognized a need for cyber investigation training but the majority felt they did not have the ability or understanding to investigate a cyber related offense without help From an outside agency. Of the forty agencies surveyed, ten agencies (25%) reported to have individuals dedicated to, or specializing in, the investigation of cyber related offenses and who have received specialized training in the area of cyber investigation. Of the ten agencies reported to have received specialized training only seven agencies (5.7%) felt they could investigate a cyber related offense without the help of an outside agency (Figure 1). As more agencies gain more experience and training in cyber investigation the area of confidence is expected to rise.

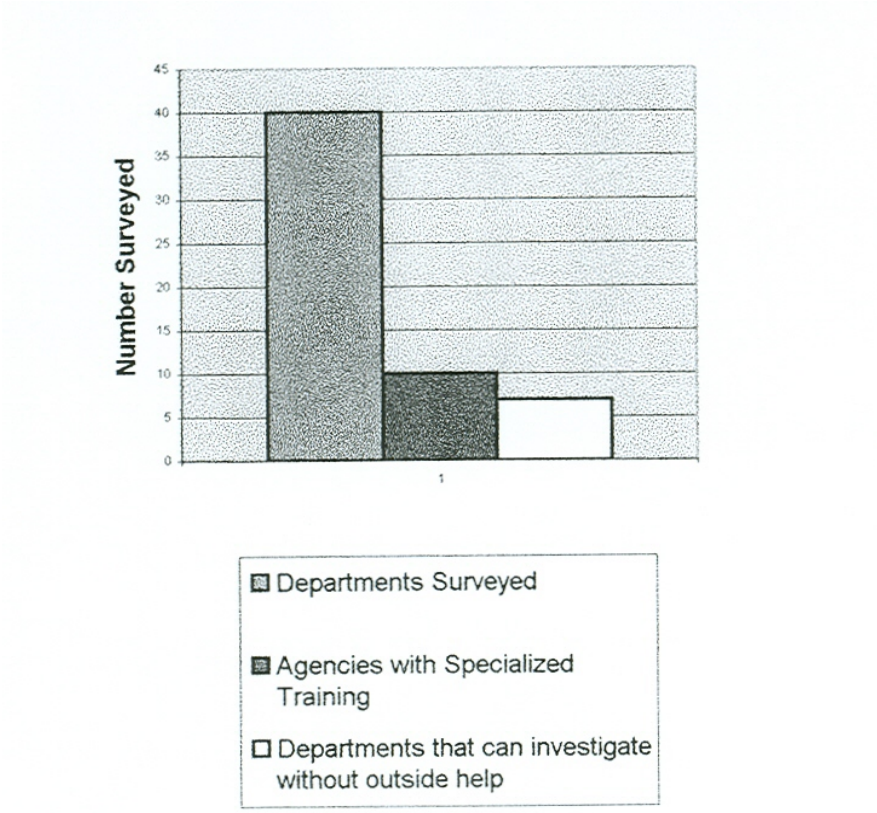

Figure 1

Survey of Cyber Investigation Ability

While reviewing the respondents information it was noticed that the individuals who felt their department could investigate a cyber crime satisfactory were associated with some form of a Cyber task force typically over seen by a federal or state agency.

CONCLUSION

Cyber crimes are here to stay. They cannot be stopped without education, awareness and training. What has been lacking is the willingness to employ the existing resources to meet the challenge. The abundance of computers in every sector and most residences have made it

possible for most anyone to access this technology and infiltrate other cyber systems. The lone computer perpetrator and technocrats, void of ethics, will for years to come prey on our electronic society. Armed with the knowledge and occupying a position of trust, they will continue to harass the electronic airways with impunity. Cyber crime can be prevented, although the effort and precautions necessary may not be deemed worthwhile to the individual or business entity until after they have fallen victim to a cyber crime.

Training and education of law enforcement personnel can help restore the confidentiality and integrity of the system once it has been compromised and aid in the prosecution of a case. By informing the victim of preventive measures, law enforcement can aid to deter repeat offenses. Employees should be made aware of the policies and laws associated with automation security. This would aid law enforcement in their investigation and assist in the detection of the crime.

The cyber criminal is not the super criminal our media has portrayed. The modern law enforcement officer, if properly trained can play an important role in the investigation and prosecution of a cyber crime. Identifying and understanding the crime are essential for law enforcement. Understanding the *modus operandi* of the perpetrator, and the threat they pose is an important beginning.

REFERENCES

Bequai, A. (1983) How to prevent computer crime. New York, NY: John Wiley & Sons.

Campus Crime. 10, (8) (2000 August) Silver Springs, MD: Business Publishers

Carley, W. & O'Brien, T. (1995, Sep. 12) How citicorp's system was raided and funds moved around the world. The Wall Street Journal pp.l

Clarke, R. (1998). Technological aspects of internet crime. Australian Institute for Criminology's Conference on Internet Crime, Melbourne University [On-Line] Available: http/ /www.anu.edu.au/people/Roger.Clarke/II/

Davis, J. (2001). Computer intrusion investigation guidelines. FBI Law Enforcement Bulletin, 70 (1) pp. 8

Economic crime prevention technological bulletin, (2001) [On-line]. Available: http: http://ww.rempgrc.gc.ca/html/ccprev.htr

Gibson, S. (2001). The escalating threat of internet denial of service. [On-line]. Available: http://grc.com/dos/PacketRouting.htm

Grolier Electronic Publishing, Inc. (1992). White-collar crime. [On-line]. Available: http://www.Grolier.com

Guy, E. (2000, Feb. 21). Cyber crimes. Business Week,, pp. 36

United Nations manual on the prevention and control of computer related crime, (NOS 43 & 44) [On-line]. Available: http://www.ifs.univie.ac.at/-pr2gq/rev4344.htm

Lormel, D. & Johnston R. (2001). Internet crime: Is your agency ready to respond, Police Chief, 68, (5) pp. 66

Nathan, S., Hutto, S. & Fromm, K. (1992). Understanding computers. Alameda, CA: SYBEX

Pettinari, D. (2001) Cybercops, just a click away at the internet fraud center. Police Futurists, 8, (3). pp. 8

School of Information Warfare and Strategy. (1995) Definitions for the discipline of information warfare and strategy. Washington D.C.: National Defense University

State Farm Fire and Casualty (1997). The iceberg crime. [Brochure] Bloomington, IL

Thomas, T. (1996-97), Deterring information warfare: A new strategic challenge, [Online]. Available: http//call.army.mil/call/fmso/fmsopubs/issues/deteriw.htm

Appendix 1

Agencies Surveyed

Abilene Police Department
Allen Police Department
Amarillo Police Department
Arlington Police Department
Austin Police Department
Brazos County Sheriff's Department
Collin County Sheriff s Office
Conroe Independent School District Police Department
Converse Police Department
Corpus Christie Police Department
Dalhart Police Department
Del Rio Police Department
Department of Public Safety - D/FW Airport
Desoto Police Department
El Paso Police Department
Farmers Branch Police Department
Galveston County Sheriff's Office
Grapevine Police Department
Greenville Police Department
Harker Heights Police Department
Houston Independent School District
Humble Police Department
Lubbock Police Department
Luling Police Department
Midwestern State University
Missouri City Police Department
New Braunfels Police Department
Orange County Police Department
Pflugerville Police Department
Rockport Police Department
San Antonio Police Department
Spring Branch Independent School District Police Department
Temple Police Department
Texas Commission of Law Enforcement Officers Standards and Education
Texas State Technical College
Travis County Sheriff's Office
Tyler Police Department
University of Texas Police Department - Houston
Webster Police Department
Wichita Falls Police Department

Appendix 2

Survey

1. Type of department:____Municipality ____County____ISD____University _____Other

2. Population of jurisdiction: (estimate if necessary)_____

3. Number of officers in your department (authorized):_____

4. Number of investigators in your department (authorized):_____

5. Does your department have a division or individual specializing in computer related offenses. _____YES _____NO

6. Is any special training provided or required. If so, what type? (Answer only if #5 is YES)

7. How would you rate your department's understanding/ability to investigate Computer Related Offenses without help from an outside agency? (Circle)

Satisfactory Unsatisfactory

Department: _____

_____